HaystackID®

Detecting the Undetectable: Deepfakes Under the Digital Forensic Microscope

Educational Webcast

08 | 06 | 2025

HAYSTACK®

Agenda

1. What is a Deepfake?
2. Threat Landscape
3. Abuse Types and Consequences
4. Trust Crisis in the Age of AI
5. Detection Red Flags
6. Forensic Techniques and Tools
7. AI-Powered Solutions
8. Legal Challenges and Admissibility
9. Key Takeaways and Q&A

HAYSTACK

John Wilson

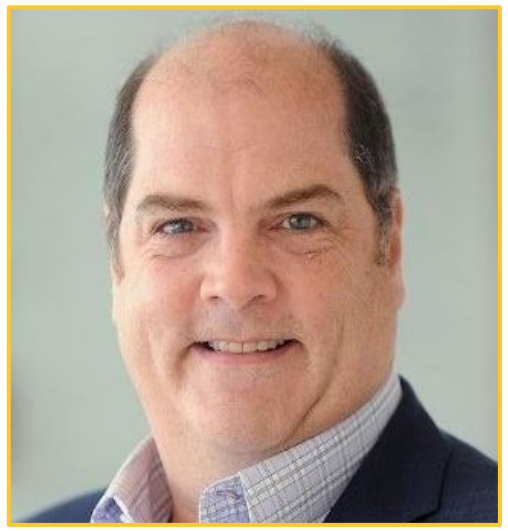
Chief Information Security Officer and President of Forensics HaystackID

As Chief Information Security Officer and President of Forensics at HaystackID, **John Wilson** provides consulting and forensic services to help companies address various matters related to electronic discovery and computer forensics, including leading forensic investigations, cryptocurrency investigations, and ensuring proper preservation of evidence items and chain of custody. He regularly develops forensic workflows and processes for clients ranging from major financial institutions to governmental departments, including Fortune 500 companies and Am Law 100 law firms.

HAYSTACK

Todd Tabor

Senior Vice President of Forensics
HaystackID



In 2021, **Todd Tabor** joined HaystackID and is currently the Senior Vice President of Forensics. In this role, he is responsible for the day-to-day operations of HaystackID's Forensic Team as well as developing the processes and procedures of that team. Prior to joining HaystackID, Todd was the Executive Vice President of Operations for Veristar.

Rene Novoa

Vice President of Forensics
HaystackID

As Vice President of Forensics at HaystackID, **Rene Novoa** brings over two decades of experience in technology, specializing in data recovery, digital forensics, eDiscovery, and client engagement. Based in Chicago, he leads the company's forensic lab with a focus on innovation and emerging technologies. Rene plays a key role in advancing the capabilities of HaystackID's forensic team by driving research and development initiatives that address both current and future technology challenges.

HaystackID Overview

HaystackID® is a leading provider of specialized data services that solve complex challenges across legal, compliance, regulatory, and cyber domains. We help law firms and corporate legal departments manage information effectively throughout the data lifecycle. Known for our innovation, precision, and commitment to security, HaystackID empowers legal teams to address **data gravity**, where information demands action, and **workflow gravity**, where critical requirements demand coordinated expertise.

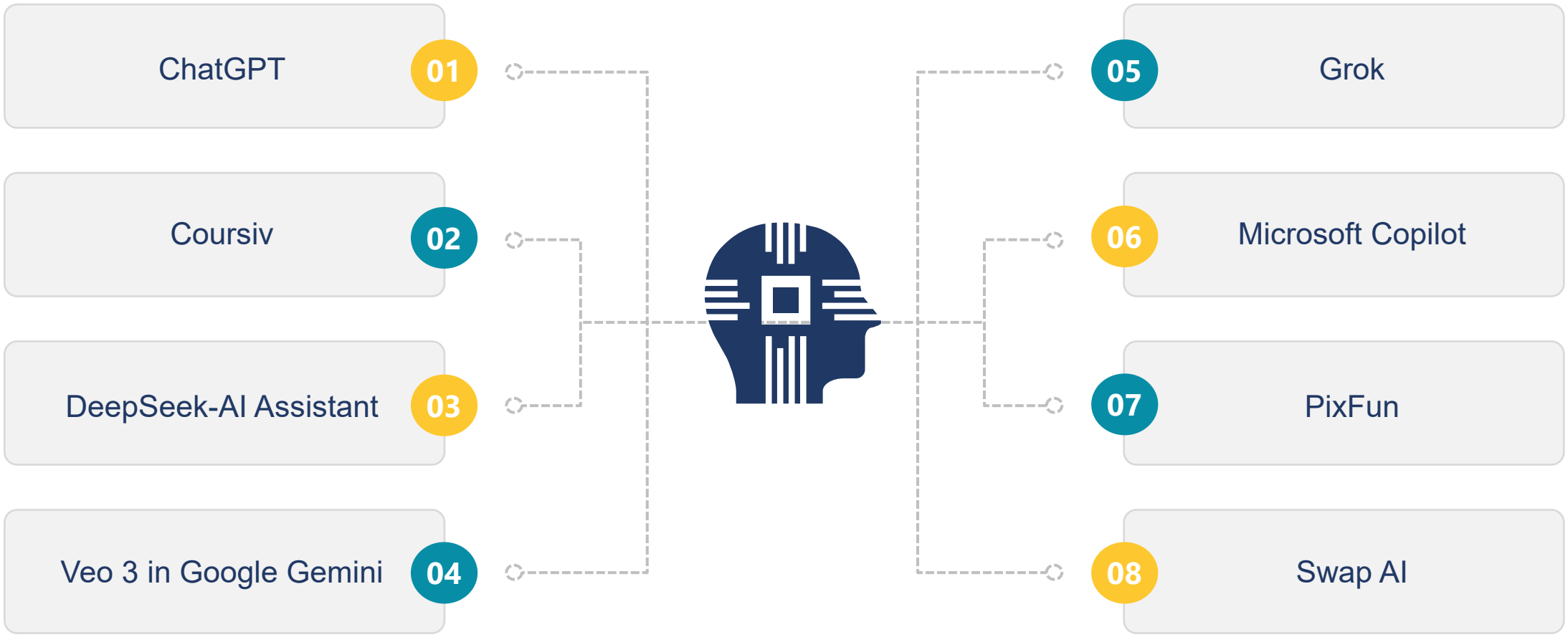
Recognized globally by leaders including Chambers, Gartner, IDC, and Legaltech News, HaystackID delivers integrated solutions spanning expert advisory, cybersecurity, AI-driven discovery, and scalable review—supported by our unified CoreFlex™ service interface. With a continual focus on security, privacy, and integrity, HaystackID enables legal and compliance professionals to operate with confidence in an increasingly complex digital landscape.

The Deepfake Threat Landscape

What We Typically Think of As a Deepfake

- A **deepfake** is a type of synthetic media created using artificial intelligence, particularly deep learning techniques like **Generative Adversarial Networks (GANs)**, to manipulate or generate visual and audio content that appears authentic.
- **In simple terms**, A deepfake is a fake video, image, or audio clip that **realistically mimics a person's likeness or voice**, making it seem like they did or said something they never actually did.

How Deepfakes Are Made



For the Gram!

Fun with Action Figures and Mature Looks

Rene

Action Figure Rene

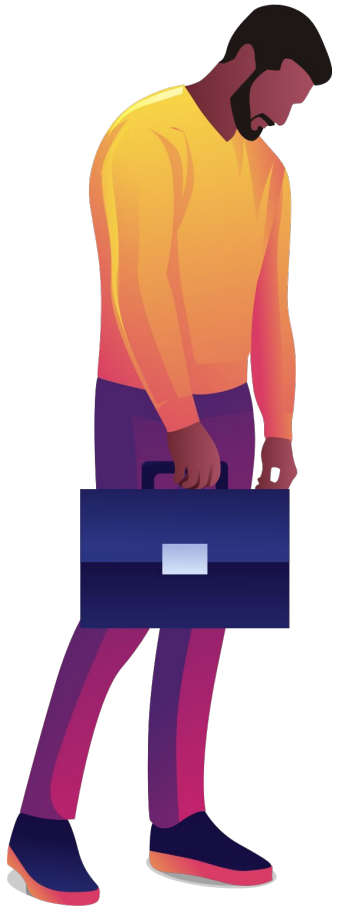
Old Man Rene

Photo and Video Fun

Types of Deepfake Abuse

- Sexually Explicit Deepfakes
- Financial Extortion
- Defamation and Misinformation
- Impersonation and Identity Theft

Consequences of Abuse



- **Psychological Distress:** Victims often experience significant psychological and emotional harm, including anxiety, depression, and feelings of shame and humiliation.
- **Reputational Damage:** Deepfakes, particularly sexually explicit ones, can inflict irreparable harm to a victim's reputation, affecting their personal and professional life.
- **Social Isolation and Trauma:** Victims may withdraw from social interactions and face difficulties in building and maintaining healthy relationships, further exacerbating emotional distress.
- **Fear and Intimidation:** The presence of deepfakes can lead to constant fear and anxiety, as victims worry about the content resurfacing or being exploited further.

The Trust Crisis in the Age of AI

“Think before you trust.” The core threat isn't the tech — it's the **manipulation of trust**.

$200M+ loss in Q1 alone from deepfake-enabled fraud.

Attacks target **emotional manipulation**, not just systems.

Psychology > Technology — familiarity is the vulnerability.

HAYSTACK

The Threat Landscape

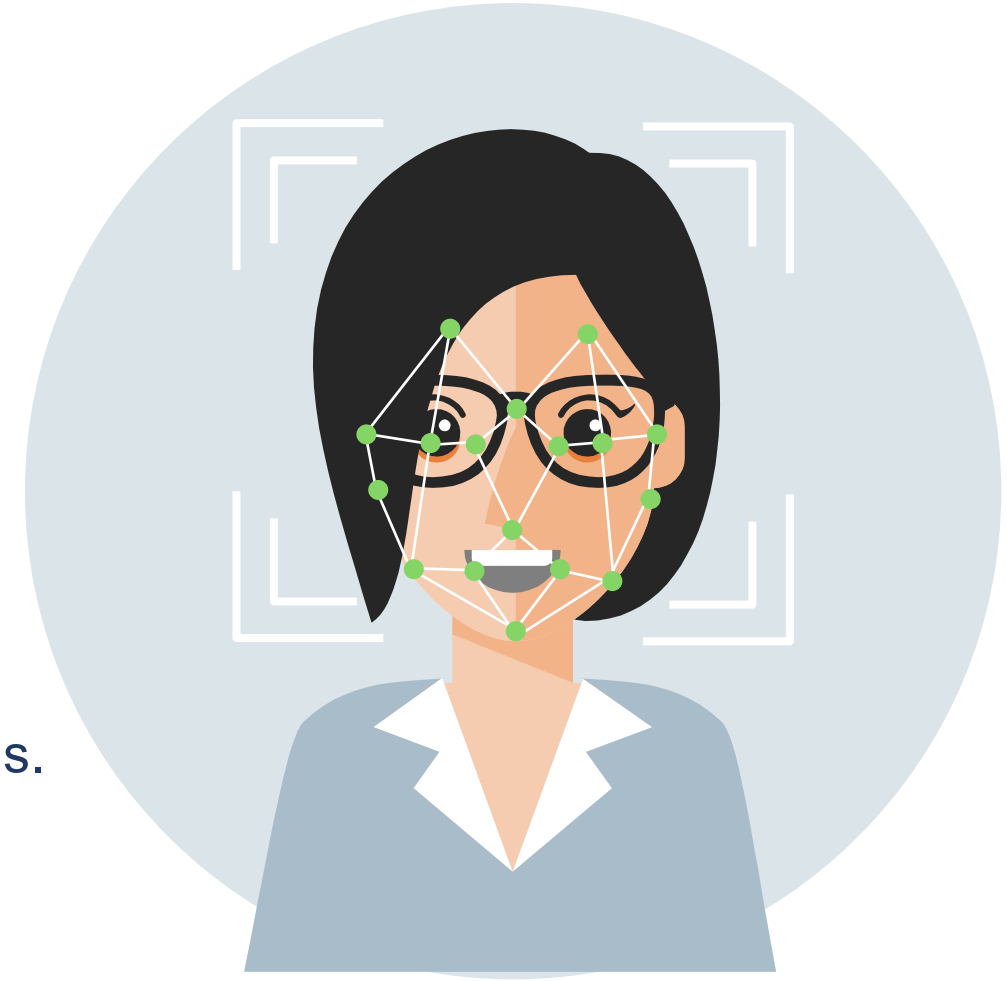
Nation States to Teen Scams!

Examples of Abuse

- **Voice cloning:** Senators Ben Cardin (Sept. 2024) and Marco Rubio (July 2025).
- **Fake advisors:** Susie Wiles (May 2025).
- **Italy:** Deepfake kidnapping for ransom.
- **Singapore:** Blackmail of cabinet ministers.

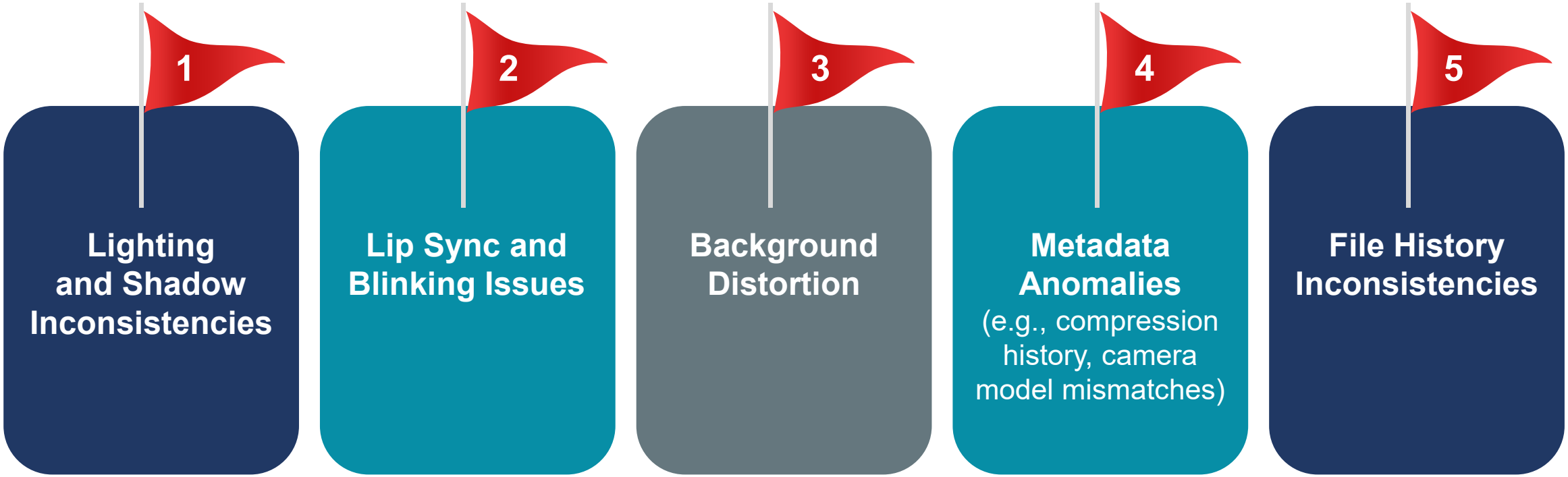
Dark Use Cases

- North Korean operatives hired into 300+ US tech firms.
- Romance scams targeting:
  - **Teen boys (13–19)** via coordinated team scams.
  - **Elderly (70+),** often leading to **suicide risks.**

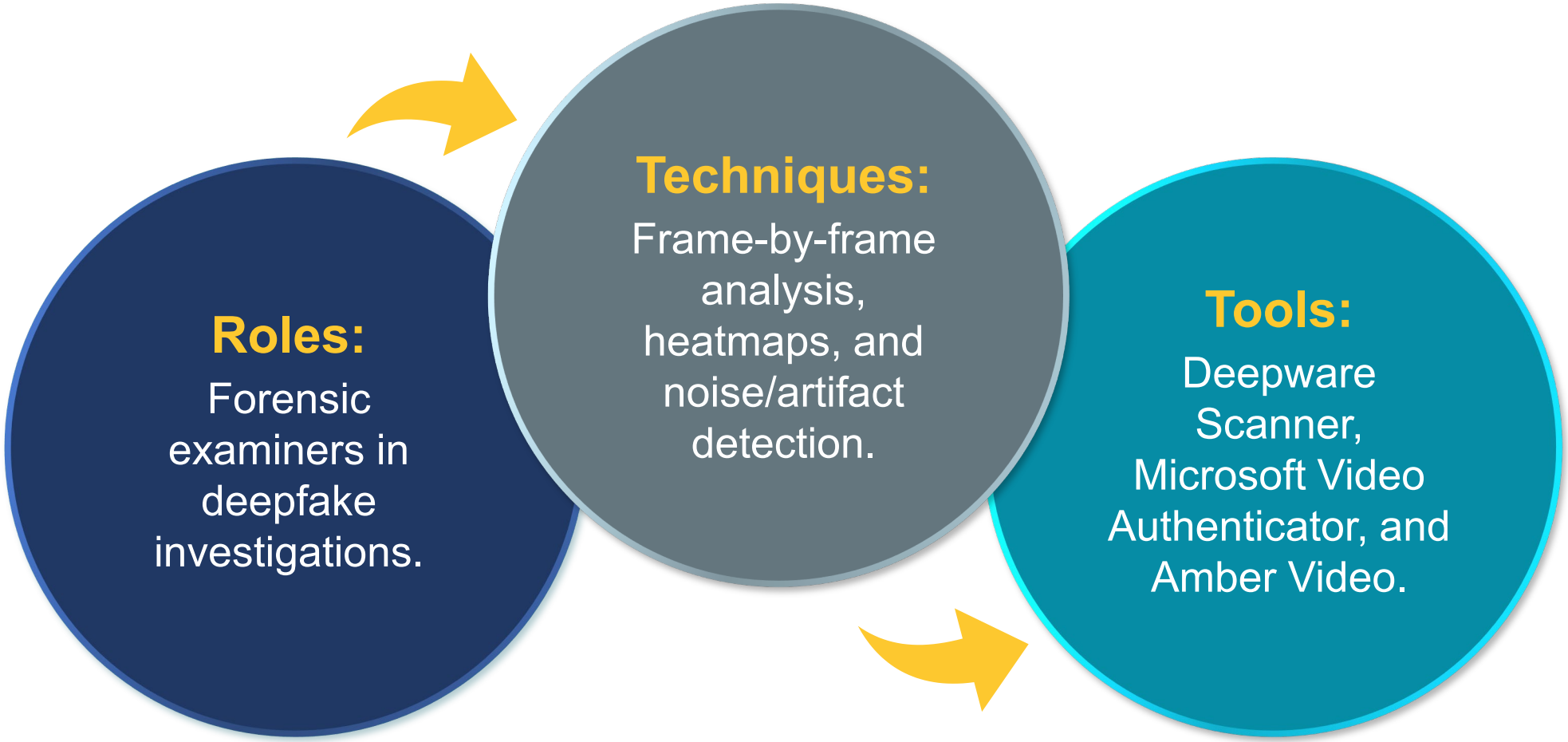


HAYSTACK

Red Flags and Practical Detection Cues

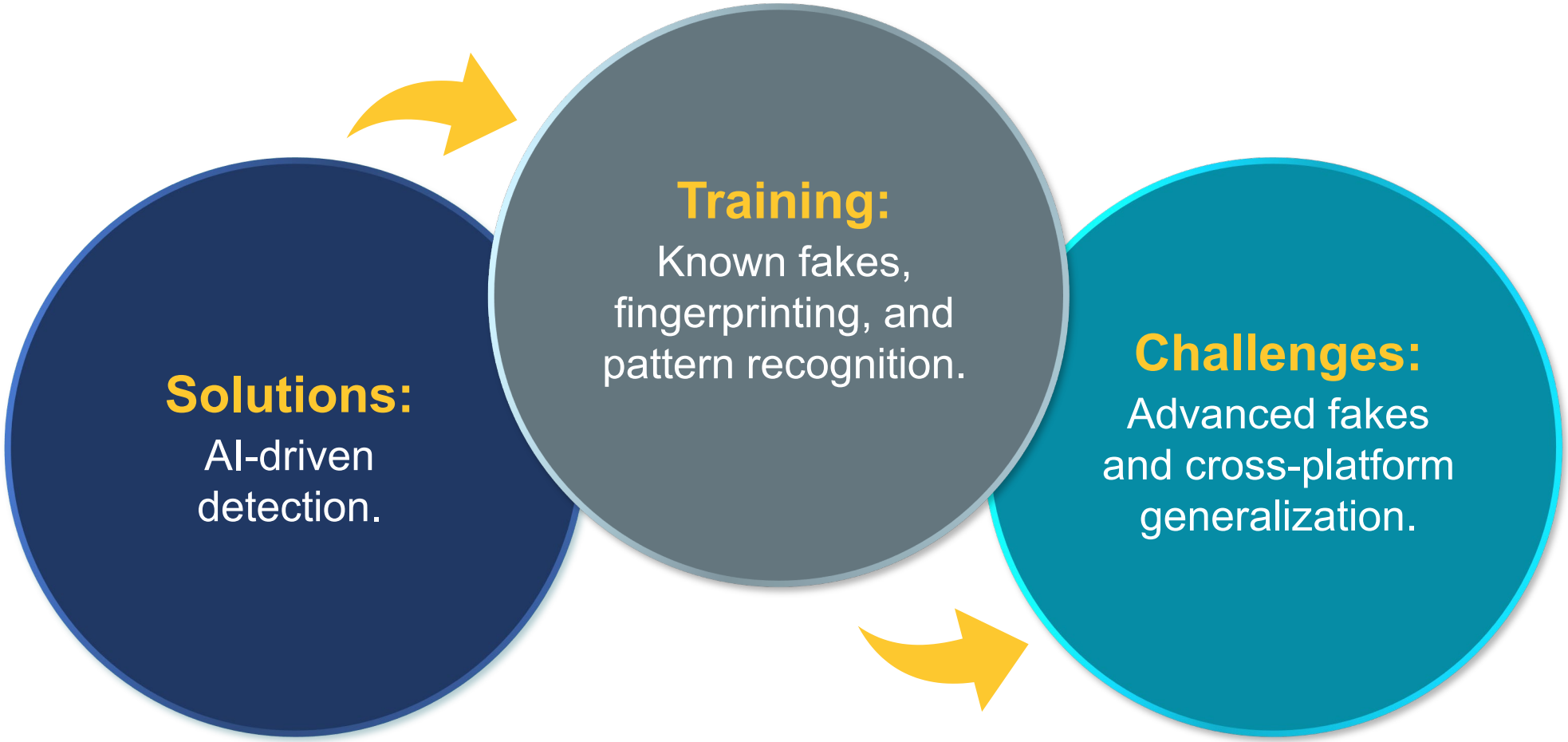


Digital Forensics in Action



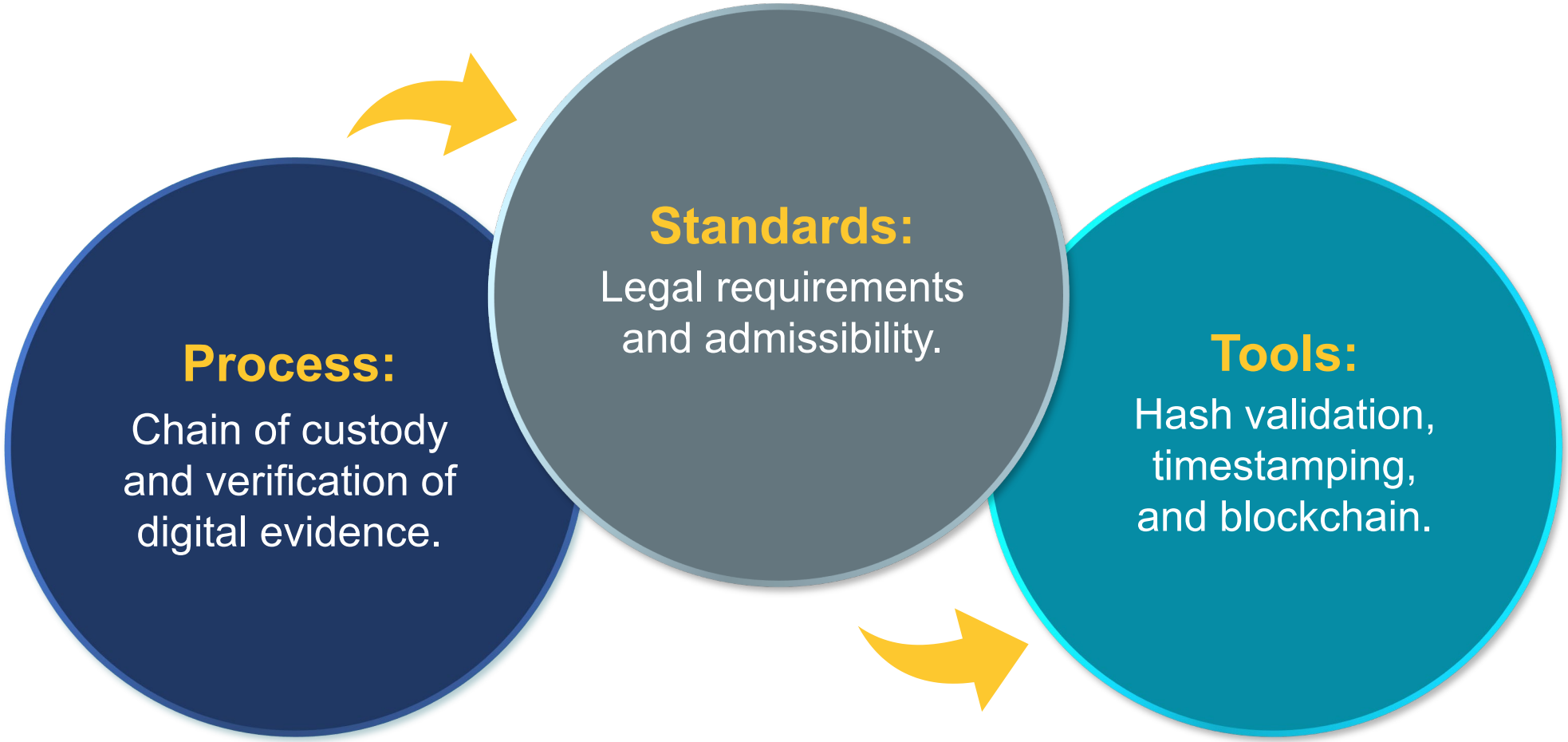
HAYSTACK

AI-Powered Deepfake Detection Tools



HAYSTACK

Ensuring Authenticity and Admissibility



Authenticity Is No Longer Assumed

- Educating legal teams and investigators.
- Integrating tools into early case assessment.
- Coordinating with tech vendors.
- Preparing expert testimony.
- Fake evidence in chat threads, contracts, and citations.
- Deepfakes cited in false cases—**no current forensic standard**.
- Courts struggle with **admissibility** and **defining experts**.
- **Risks**:
  - No trust upload mechanism.
  - No verified forensic chain of custody.
  - Content authentication standards lagging.

HAYSTACK

Key Takeaways

1. Deepfakes are a growing **threat** to truth and trust.
2. They can be used to attack our **psychology** and **mental well-being**.
3. Detection is possible with **tools** and **expertise**.
4. Forensic analysis is needed for **validation** and **defensibility**.
5. Continuous **learning** and **collaboration** are essential with both private and public agencies.

Questions?

Learn how we can help you at HaystackID.com
or reach out to us at Info@HaystackID.com / 800.267.9695

HAYSTACK®